RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: TPV-T10

Break Glass: MSPs and SMBs Can't Survive on Corpsec Rules

Tarah Wheeler, CISA, CISSP, GIAC GXPN, GIAC GMOB, GED

CEO & Founder
Red Queen Dynamics
https://www.linkedin.com/in/tarah/

Matt Lee, CISSP, CCSP, CFR, PNPT, CCSK, CCZT

Security and Compliance Senior Director
Pax8
https://www.linkedin.com/in/cybermattlee/

RSAC™ 2025 Conference

Many Voices.
One Community.

Matt Lee, CISSP, CCSP, CFR, PNPT, CCSK, CCZT

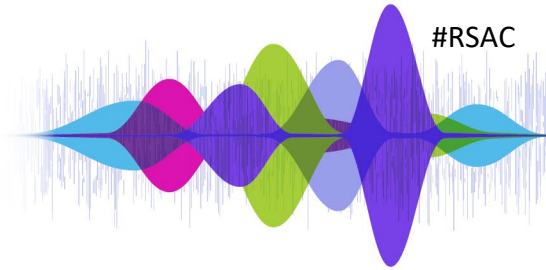
Security and Compliance Senior Director
Pax8
https://www.linkedin.com/in/cybermattlee/

RSAC™ 2025 Conference

Tarah Wheeler, CISA, CISSP, GIAC GXPN, GIAC GMOB, GED

CEO & Founder
Red Queen Dynamics
https://www.linkedin.com/in/tarah/

Many Voices.
One Community.



Disclaimer

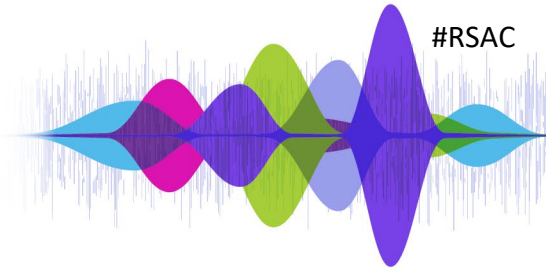
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Session Overview

- Outline of the three major focus areas
  - Enterprise vs SMB Economy Gap
  - MSP Creative Hacks and unconventional Solutions
  - Bridging the Gap, practical solutions



Session Overview

- What attendees will learn and take away
  - Traditional enterprise security rules break down at the SMB level
  - MSPs Serving SMBs employ creative but unconventional security practices
  - Enterprise can bridge the gap with SMBs by asking better risk questions, of the CORRECT party, the MSP

RSAC 2025 Conference

1: THE ENTERPRISE VS. SMB ECONOMY GAP

CLIENT
EXPECTATIONS
CLIENT
BUDGET

RSAC 2025 Conference

Enterprise Security Assumptions

- Internally managed IT departments
- Dedicated security personnel
- Corporate-owned and managed devices
- Risk Management Dominates vs Cost Management

RSAC 2025 Conference

How do SMBs deal with security?

RED QUEEN pax8

The Cyber Security Poverty Line

RED QUEEN pax8

RSAC 2025 Conference

Counts by Annual Sales (Updated 2023-03-30)

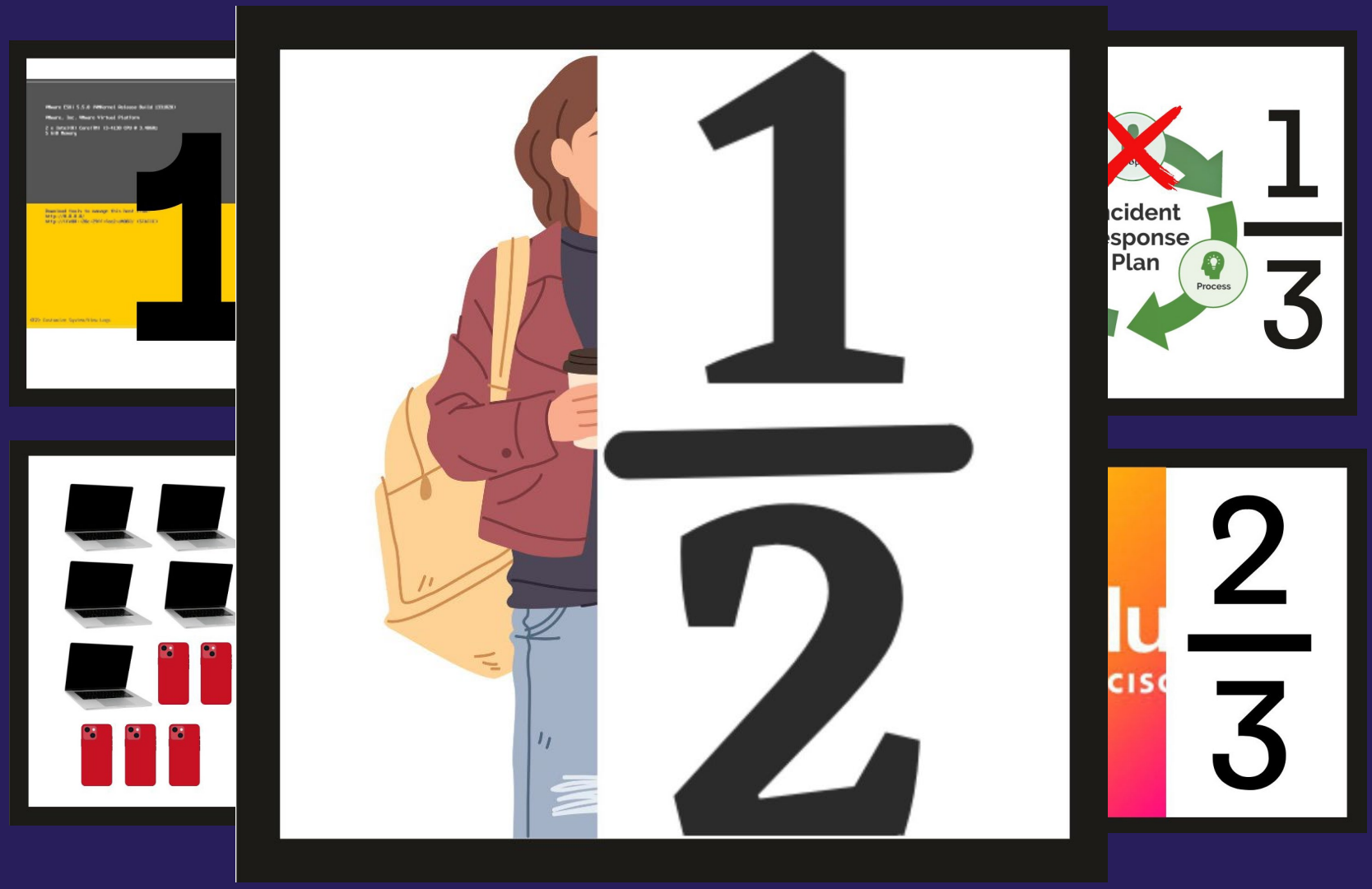
Annual Sales Ranges	Number of Businesses
Under 500,000	14,382,087
500,000 - 999,999	818,345
1,000,000 - 2,499,999	559,315
2,500,000 - 4,999,999	226,121
5,000,000 - 9,999,999	148,583
10,000,000 - 99,999,999	181,386
100,000,000 - 499,999,999	24,708
500,000,000 - 999,999,999	4,174
1,000,000,000+	5,334
Uncoded records	1,882,514
Grand Total	18,232,567

6-7% TOPLINE REVENUE FOR TECH ON AVERAGE

- 98% OF COMPANIES HAVE <100 EMPLOYEES
- 89% <20 EMPLOYEES
- WHAT WOULD THOSE COMPANIES DO FOR IT?

https://avasant.com/report/it-spending-as-a-percentage-of-revenue-by-industry-company-size-and-region/
https://www.naics.com/business-lists/counts-by-company-size/

RSAC 2025 Conference



Tarah, what can you buy for $50,000 in Cyber security?

RED QUEEN pax8

RSAC 2025 Conference

SMB Reality Check

- Limited resources (financial, personnel, expertise)
- Focus on core business functions, not security
- IT as a utility, not a strategic investment (“It’s a cost center, stupid”)
- MSP outsourcing is the primary way SMBs solve this economics challenge

RSAC 2025 Conference

Knowledge Asymmetry

- Why SMBs can't "just learn" enterprise security
- Parallel to legal or financial expertise
- “Security Poverty Line” (Money, Expertise, Capability, and Influence)

RSAC 2025 Conference

The SMB Market Represents 44% Of All Tech Spend And Is 80% Partner-Delivered

Jay McBain
Chief Analyst - Channels, Partnerships & Ecosystems - Canalys - Channel Influencer of the Year

109 articles ✓ Following

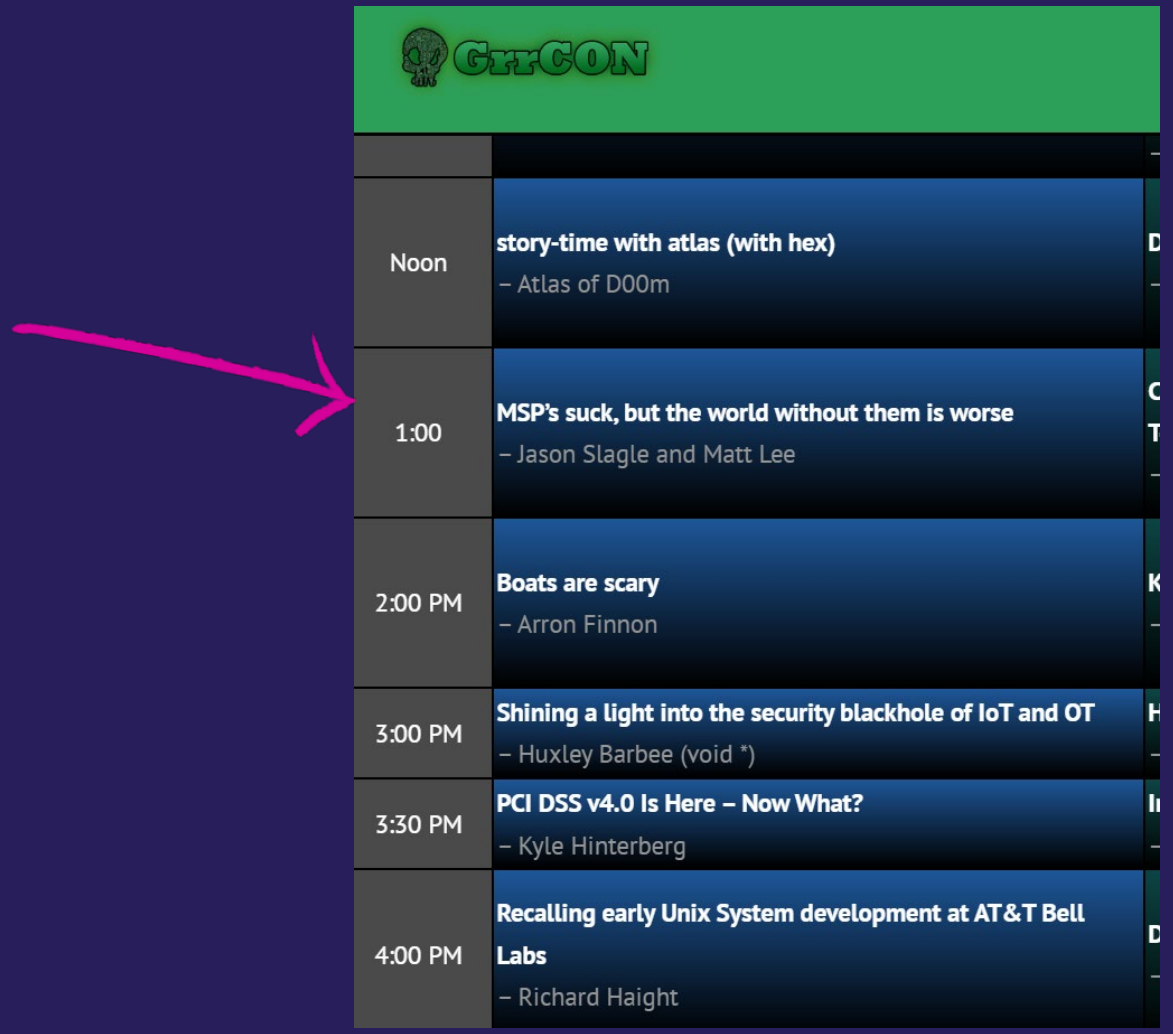
September 13, 2023

RED QUEEN pax8

RSAC 2025 Conference

MSP ≠ MSP

RSAC 2025 Conference



GrrCON

Noon	**story-time with atlas (with hex)** – Atlas of D00m
1:00	**MSP's suck, but the world without them is worse** – Jason Slagle and Matt Lee
2:00 PM	**Boats are scary** – Arron Finnon
3:00 PM	**Shining a light into the security blackhole of IoT and OT** – Huxley Barbee (void *)
3:30 PM	**PCI DSS v4.0 Is Here – Now What?** – Kyle Hinterberg
4:00 PM	**Recalling early Unix System development at AT&T Bell Labs** – Richard Haight

RSAC 2025 Conference

MSP Landscape Positives

- MSPs often are a “economy of scale” option for SMB
- MSPs bring process as a result of efficiency being the only way to profit
- The tools and protections are significantly better than an SMB alone would utilize, even at the worst.
- They are there because they LOVE their clients, communities, and KNOW their clients’ business.

RED QUEEN pax8

RSAC™ 2025 Conference

RSAC 2025 Conference

MSP Landscape Drawbacks

- MSPs are often in only geo territories
- MSPs are themselves quite below the security poverty line, many of them functioning on the same SMB numbers we spoke of earlier
- MSPs being small staff typically under 30 employees, they themselves are subject to SMB forces, low pay, high workload, little profit.
- There is no barrier to be an MSP

RSAC 2025 Conference

The SMB / MSP Compliance Paradox

- Enterprise compliance frameworks (SOC 2, ISO 27001, etc.)
- SMB interpretation and application - at best they're doing CMMC level 1, at worst, "doesn't my MSP do that shit?"
- This creates a risk "Gap" between compliance checks of risk posture for your Enterprise, and the reality of your Risk from those SMBs.
- This comprehension gap leads to implementation gaps. They check the box, but it is not actually done. Knowledge asyncronicity causing risk measurement uncertainty.

RED QUEEN pax8

RSAC 2025 Conference

Risk Perception Differences

- How SMBs view security risks vs. enterprises (“I’m too small to be worth hacking”)
- Business impact calculation differences
- Cost-benefit analysis through SMB lens

RSAC 2025 Conference

2: MSP CREATIVE HACKS AND UNCONVENTIONAL SOLUTIONS

RSAC 2025 Conference

Enterprise

vs

MSP

RSAC 2025 Conference

MSP Resource Constraints

- Typical MSP endpoint to tech ratio – ~350-700:1
- Time segmentation and allocation challenges
- Profit margins and the reality of the security world escalating asymptotically

RSAC 2025 Conference

MSP vs Ent. engineer workload

RED QUEEN pax8

RSAC 2025 Conference

DAP to GDAP

RSAC 2025 Conference

The “Break Glass” ish.. admin… Account

RED QUEEN pax8

RSAC 2025 Conference

Break Glass Account

Enterprise

- Exist as last measure use for systems in crisis
- Any time one is used, alarms go off
- Use is highly restricted to POLP

MSP

- Used on the daily to solve issues with multi tenancy, and business challenges
- They would be annoyed if they were notified, and the MSPs often do NOT monitor or audit use
- All MSP employees often have access on hire

RSAC 2025 Conference

MFA

Enterprise

- Absolutely required, no excuses
- SSO used widely with risk-based CA
- Largely fall on the side of security over convenience
- Strict 1:1 MFA for human identities

MSP

- Extreme variance, BYOD, Hearts and Minds, Risk Tolerance, License costs, etc
- Often NO escalation for riskier actions
- More concern with potential account lockout than account compromise.
- Often come up with “Creative solutions” such as sharing TOTP seed codes, storing passwords WITH the TOTP codes, etc

RSAC 2025 Conference

Password Management

Enterprise

- Good adoption of SSO reduces number of Password type access instances.
- Passwords are stored in vaults with complexity, and re-use requirements
- Largely fall on the side of security over convenience
- Strict 1:1 MFA for human identities

MSP

- Common to share password vaults with little tracking of use
- Little to no “One time Pad” approach, no password rotation on use
- Most employees of MSP have access to ALL client creds from day 1
- Use algorithmic passwords such as last 4 of phone, 3 letter company identifier, first 3 of phone, plus !

RED QUEEN pax8

RSAC 2025 Conference

Risk Management

Enterprise

- Good adoption of SSO reduces number of Password type access instances.
- Passwords are stored in vaults with complexity, and re-use requirements
- Largely fall on the side of security over convenience
- Strict 1:1 MFA for human identities

MSP

- Common to share password vaults with little tracking of use
- Little to no “One time Pad” approach, no password rotation on use
- Most employees of MSP have access to ALL client creds from day 1
- Use algorithmic passwords such as last 4 of phone, 3 letter company identifier, first 3 of phone, plus !

RED QUEEN pax8

RSAC 2025 Conference

And……

- Remote Access
- Email Security
- Backup and Recovery
- Patch and Vuln Management
- Network Security
- Cloud Security
- Security Monitoring
- Compliance Management
- Vendor Management / TPRM
- Shared Responsibility
- *Ad Nauseam……*

RSAC 2025 Conference

3: BRIDGING THE GAP - PRACTICAL SOLUTIONS

Many Voices.
One Community.

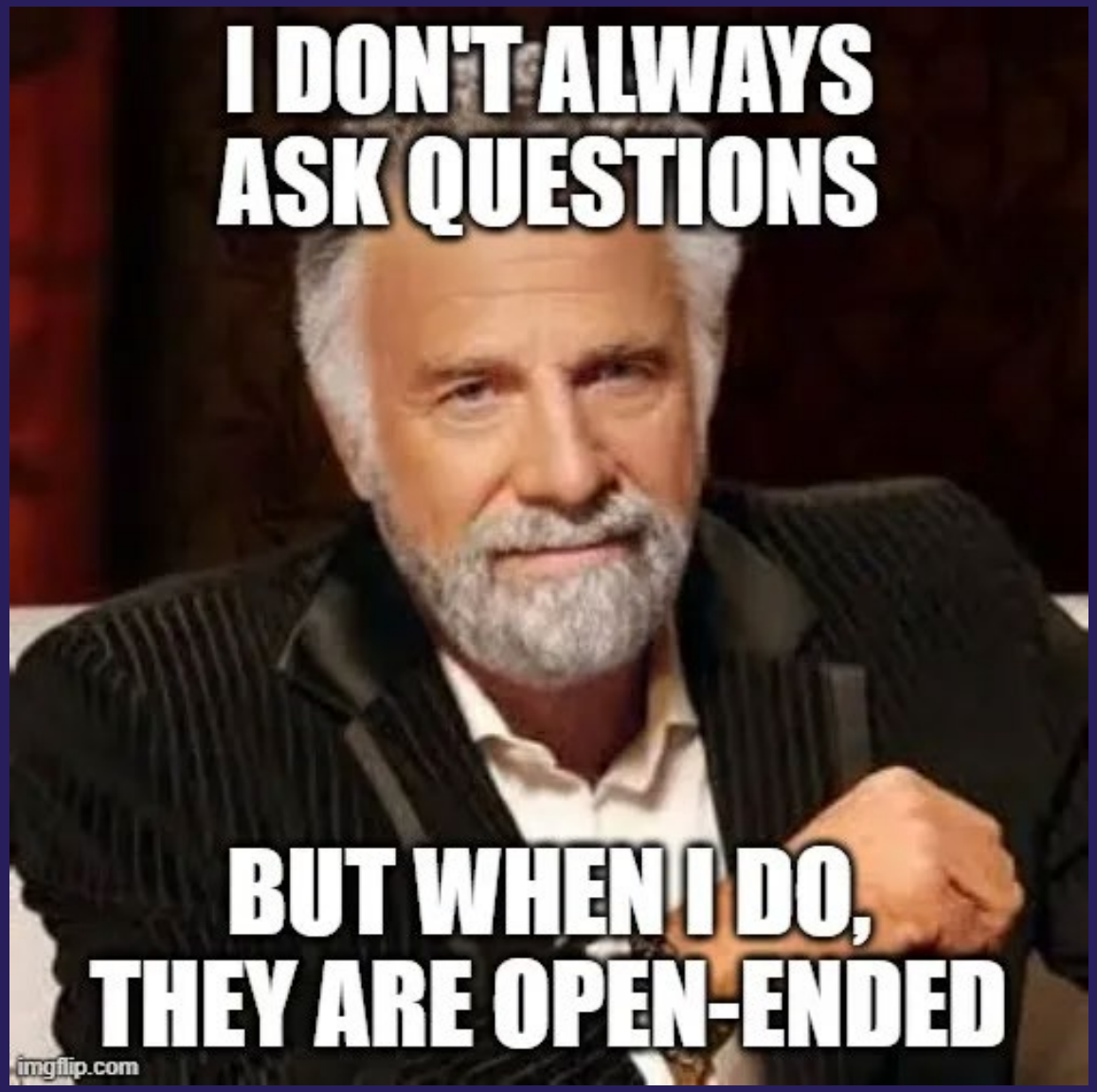
RSAC 2025 Conference

Principle of LESS privilege

RSAC 2025 Conference

RED QUEEN pax8

RSAC 2025 Conference



RED QUEEN pax8

RSAC 2025 Conference

innovate CYBERSECURITY NEWS & FEATURES THREAT ADVISORIES CYBERSECURITY EDUCATION RE

A Practical Approach to Finding Secure SMB Partners

October 29, 2024 14:02 GMT

Matt Lee, Security and Compliance Senior Director at Pax8, opened his presentation at the 2024 Nashville Innovate event with an origin story that sets the stage for his career in cybersecurity—along with a few gems of advice.

"How did I get here? I got punched in the face really, really hard..... Ultimately, it gave me the passion to dig in and try to change this world, to try to drive toward regulatory modes, education, to increase the skills of people who live below the cybersecurity poverty line's capabilities."

RED QUEEN pax8

https://innovatecybersecurity.com/news/a-practical-approach-to-finding-secure-smb-partners/

RSAC 2025 Conference

CONTROL 1

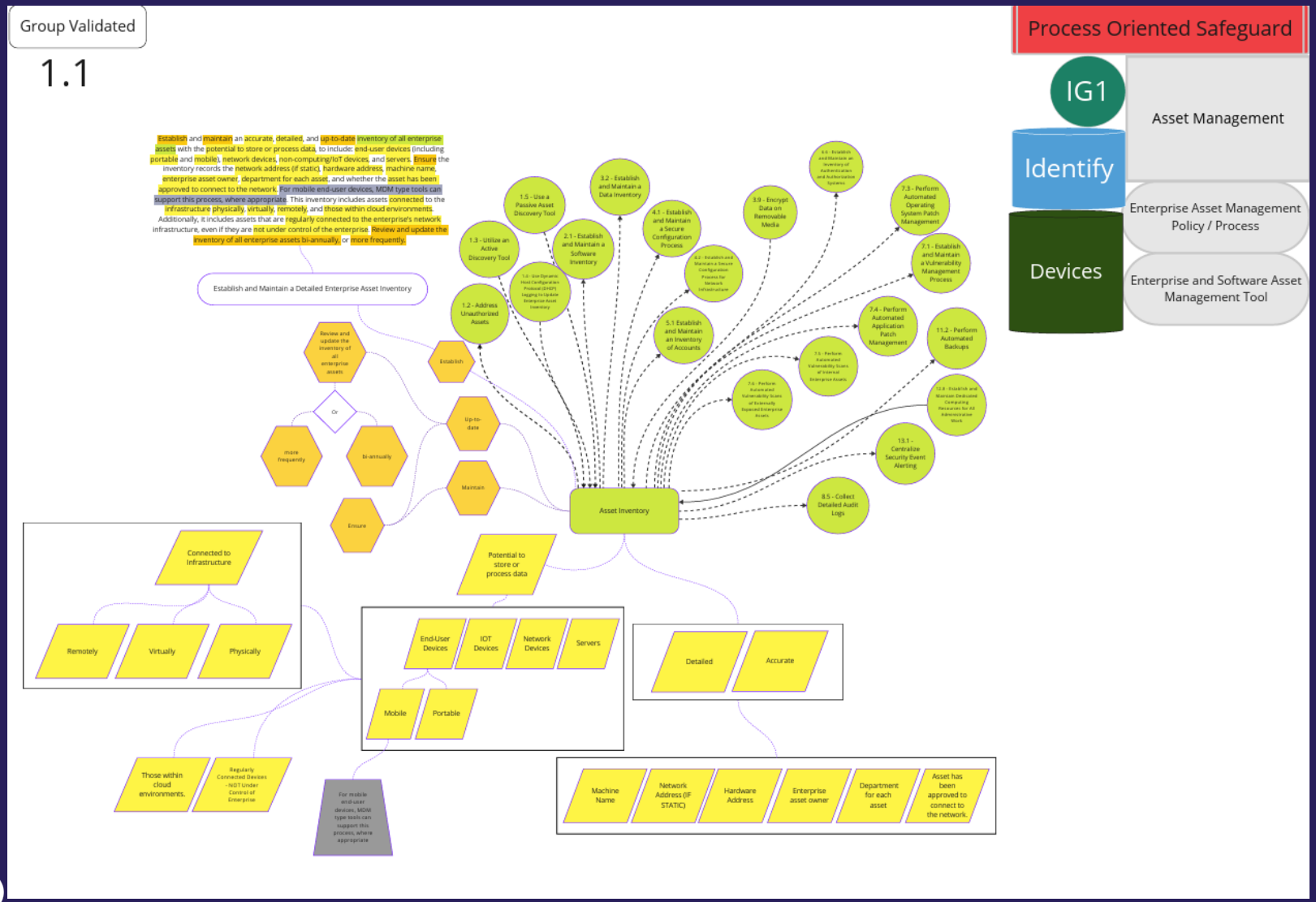
Inventory and Control of Enterprise Assets

Safeguards: 5	IG1: 2/5	IG2: 4/5	IG3: 5/5

Overview

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

RSAC 2025 Conference


Group Validated
1.1
Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.
Establish and Maintain a Detailed Enterprise Asset Inventory
Review and update the inventory of all enterprise assets
Or
more frequently
bi-annually
Ensure
Establish
up-to-date
Maintain
Asset Inventory
Connected to Infrastructure
Remotely
Virtually
Physically
Potential to store or process data
End-User Devices
IOT Devices
Network Devices
Servers
Mobile
Portable
Detailed
Accurate
Those within cloud environments.
Machine Name
Network Address (IF STATIC)
Hardware Address
Enterprise asset owner
Department for each asset
Asset has been approved to connect to the network.
1.5 - Use a Passive Asset Discovery Tool
1.3 - Utilize an Active Discovery Tool
1.2 - Address Unauthorized Assets
2.1 - Establish and Maintain a Software Inventory
3.2 - Establish and Maintain a Data Inventory
4.1 - Establish and Maintain a Secure Configuration Process
5.1 Establish and Maintain an Inventory of Accounts
3.9 - Encrypt Data on Removable Media
7.3 - Perform Automated Operating System Patch Management
7.1 - Establish and Maintain a Vulnerability Management Process
7.4 - Perform Automated Application Patch Management
11.2 - Perform Automated Backups
13.1 - Centralize Security Event Alerting
8.5 - Collect Detailed Audit Logs
Process Oriented Safeguard
IG1
Identify
Devices
Asset Management
Enterprise Asset Management Policy / Process
Enterprise and Software Asset Management Tool

RED QUEEN pax8

RSAC 2025 Conference

CONTROL 4

Secure Configuration of Enterprise Assets and Software

Safeguards: 12	IG1: 7/12	IG2: 11/12	IG3: 12/12

Overview

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

RSAC 2025 Conference

CONTROL 5

Account Management

Safeguards: 6	IG1: 4/6	IG2: 6/6	IG3: 6/6

Overview

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

RSAC 2025 Conference

CONTROL 7

Continuous Vulnerability Management

Safeguards: 7	IG1: 4/7	IG2: 7/7	IG3: 7/7

Overview

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

RSAC 2025 Conference

CONTROL 17

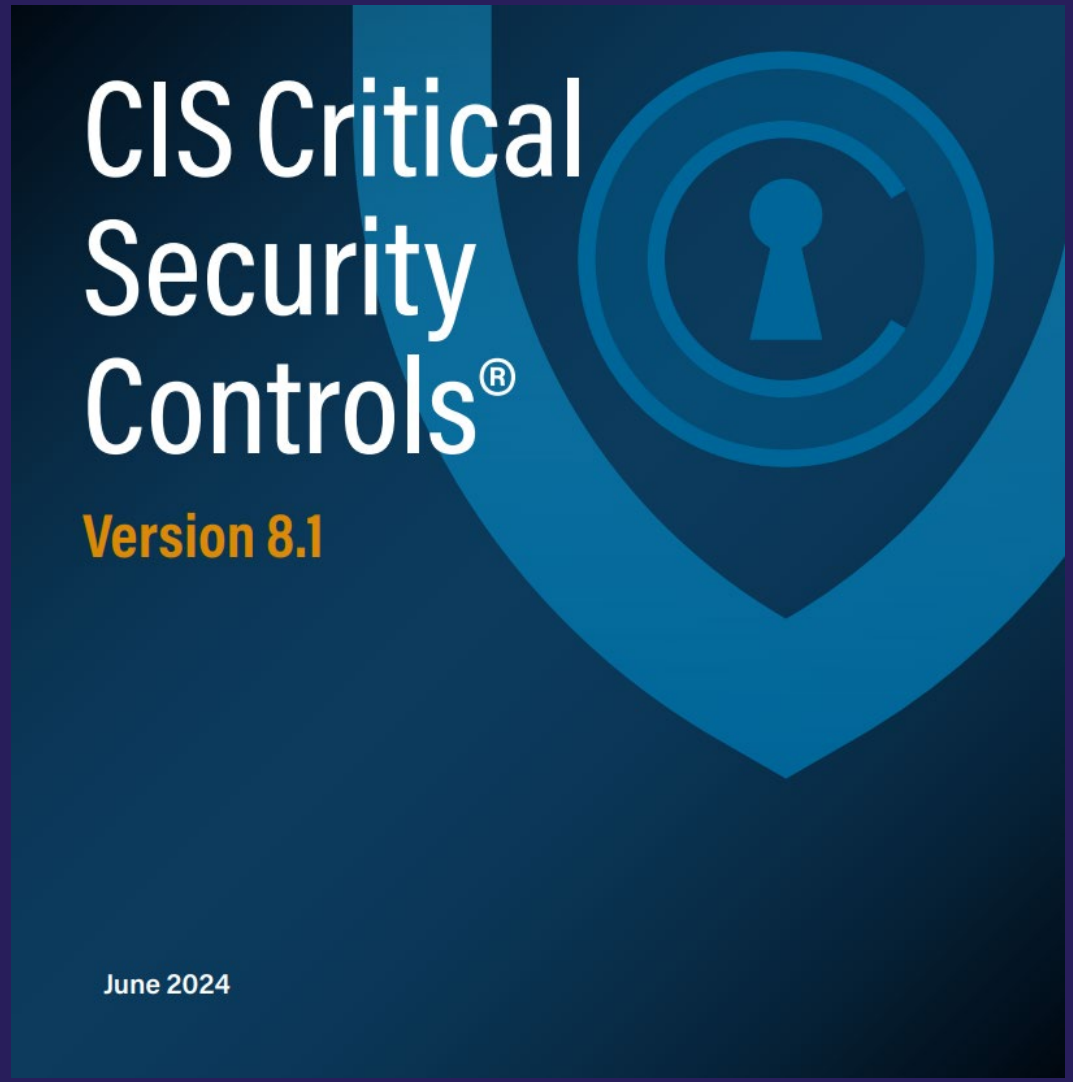
Incident Response Management

Safeguards: 9	IG1: 3/9	IG2: 8/9	IG3: 9/9

Overview

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

RSAC™ 2025 Conference



RED QUEEN pax8

RSAC 2025 Conference

KEY TAKEAWAYS

1. Traditional enterprise security rules and assumptions often break down when applied to SMBs due to fundamental differences in resources, expertise, and business priorities.

Many Voices.
One Community.

RSAC 2025 Conference

KEY TAKEAWAYS

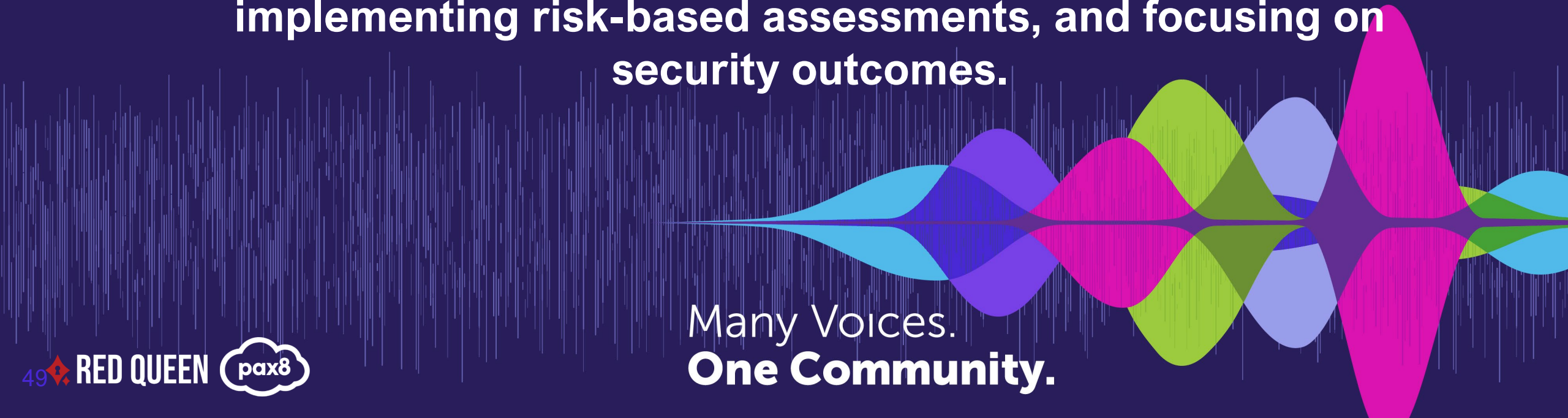
2. MSPs serving SMBs employ creative but unconventional security practices to manage their clients' needs within significant resource constraints.

Many Voices.
One Community.

RSAC 2025 Conference

KEY TAKEAWAYS

3. Enterprises can bridge the gap with their SMB vendors by adopting more realistic security expectations, implementing risk-based assessments, and focusing on security outcomes.



Many Voices.
One Community.

Making Application

- **When you return:**
  - For larger organizations:
    - Empower your supply chain!
      - Many of these organizations operate below the "cyber poverty level"
      - Helping them sort the good Service Providers from the trunk-slammers with YOUR expertise.
    - Evaluate your SMB suppliers' MSP
      - Ask open ended questions around CIS Safeguards of the MSP
        - How do you track assets for your SMB client?
        - How do you track assets for your own business, MSP?
      - Look for mature answers that cover many elements of the CIS Critical Control, safeguards
      - Ask the same open-ended question to the SMB Supplier
        - How does your MSP track your assets?
    - Compare the answers for additional insight.
    - Bonus points if you see Shared Responsibility Matrix in place as they usually are not

Making Application

- **When you return:**
  - For smaller organizations:
    - Ask your service provider if they are following a framework to guide their services and actions.
      - Look for answers like Center for Internet Security's Critical Controls, or NIST Cyber Security Framework.
    - Understand that YOU must participate in the Governance, policy, and enforcement of standards to help your Service provider MEET these capabilities.
    - Ask the same open-ended questions of your MSP
      - How are you managing the tracking of our assets?
      - Tell me about your incident response plans if I have an event.
    - Ask them how they address a shared responsibility model with you as their client. If they have an SRM they are likely already deep down the path of being awesome!

Making Application

- **When you return:**
  - For all organizations
    - Follow a framework AND understand it will always need iteration and growth.
      - Practical frameworks like the CIS Critical Controls and NIST CSF will allow for defensibility and help serve reasonableness with respect to Safe Harbor clauses like Ohio.

RSAC 2025 Conference

Many Voices.
One Community.

Q&A

Linkedin.com/in/tarah

Linkedin.com/in/cybermattlee

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!

Neither of us belong here, but colliding these worlds is our mission! We can all learn from each other!